UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/722,238	11/24/2003	Terrance A. Tomkow	RPOST-66230	6674

24201 7590 06/04/2009
FULWIDER PATTON LLP
HOWARD HUGHES CENTER
6060 CENTER DRIVE, TENTH FLOOR
LOS ANGELES, CA 90045

EXAMINER	
TAYLOR, NICHOLAS R	

ART UNIT	PAPER NUMBER
2441	

MAIL DATE	DELIVERY MODE
06/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/722,238	**Applicant(s)** TOMKOW, TERRANCE A.
	Examiner Nicholas Taylor	**Art Unit** 2441

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 have been presented for examination and are rejected.

Response to Arguments

2. Applicant's arguments filed March 27th, 2009, have been fully considered but they are deemed not persuasive.

3. In the remarks, applicant argued in substance that:

(A) The prior art of Tomkow does not teach inclusion of a pixel capable of being altered by the opening of a recipient. Instead, Tomkow only teaches a tag indicating that the message has been registered or a tag containing instructions that allow the recipient to send a registered reply. Further, the response in Tomkow is a separate email that is sent, rather than Applicant's claimed altering of the picture in the message prior to sending to the server.

As to point (A), Tomkow teaches the inclusion of a pixel capable of being altered to indicate that the message has been opened by a recipient and transmitting the message and pixel from the server to the recipient (pg. 13, lines 19-31 to pg. 14, line 10, where, e.g., a unique visible element is added at server 14 for notification that the message has been opened by a recipient, followed by transmitting the message and pixel; see further explanation in pg. 14, liens 23-31). The pixel is then altered when the message is opened at the recipient (e.g., see pg. 14, lines 30-32, followed by response of pg. 15, lines 1-3). Subsequently, both the message and the altered pixel are transmitted in response from the recipient to the server (pg. 14, lines 4-10, where the message is designed so that the notification will be returned to server 14 with both the message and pixel). Applicant has argued that a distinction exists between the tags/added message elements in Tomkow, yet it is respectfully submitted that nothing has been offered as a basis to distinguish between the two. Given the broadest reasonable interpretation of a "pixel" element, Tomkow thus reads on the present claim language.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow (WIPO Publication No. WO 01/10090 A1, published February 8th, 2001).

As per claim 1, Tomkow teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender, (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

adding a pixel to the message at the server, the pixel capable of being altered to indicate that the message has been opened by a recipient, (Tomkow, pg. 12, lines 13-28 overview; see, e.g., implementation details of pg. 13, line 19, to pg. 14, line 31, where, e.g., a unique visible element is added at server 14 for notification that the message has been opened by a recipient, followed by transmitting the message and pixel; see also further explanation in pg. 14, liens 23-31)

transmitting the message and the pixel from the server to the recipient, altering the pixel in the message when the message is opened at the recipient to indicate that the message was opened, transmitting the message and the altered pixel from the recipient to the server (e.g., see pg. 14, lines 30-32, followed by response of pg. 15, lines 1-3; see also pg. 14, lines 4-10, where the message is designed so that the notification will be returned to server 14 with both the message and pixel)

when the message is opened at the recipient, providing an encrypted hash of the message, including the indication of the opening of the message at the recipient, at the server, and transmitting the message, including the indication of the opening of the message at the recipient, and the encrypted hash to the sender (Tomkow, see pg. 22, line 14 to pg. 25, line 2, including the creation of an encrypted hash of the message with an indication of the opening of the message at the recipient; see also figs. 2E and 2F).

As per claim 2, Tomkow teaches the system further including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient and the encrypted hash of the message, and determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the message, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server).

As per claim 3, Tomkow teaches the system further including the steps at the server of:

receiving from the sender the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, hashing the message, including the indication of the opening of the message at the recipient, to provide a first digital fingerprint of the message including the indication of the opening of the message at the recipient, decrypting the encrypted hash of the message, including the indication of the message at the recipient, to provide a second digital fingerprint of the message including the indication of the opening of the message at the recipient, and comparing the first and second digital fingerprints to determine the authenticity of the message including the indication of the opening of the message at the recipient (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server, including where a first and second digital fingerprint of the message are created).

As per claim 4, Tomkow teaches the system further including the steps at the server of:

indicating to the sender the results of the comparison, and disposing of the message, and including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, when the message and the encrypted hash are transmitted by the server to the sender (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claim 5, Tomkow teaches the system further wherein the server receives the message from the sender through the internet, the server transmits the message to the recipient through the internet, the server receives the message, including the indication of the opening of the message at the recipient, through the internet, and the server transmits the message, including the indication of the opening of the message at the recipient, through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1).

As per claim 6, Tomkow teaches the system further wherein the server disposes of the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message, when the message and the encrypted hash are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claims 7 and 13, Tomkow teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender, transmitting the message from the server to the recipient through a network including at least one interim network station unknown to the sender at the time the message is transmitted, (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

the message including an alterable pixel for indicating the opening of the message at the recipient, (Tomkow, pg. 12, lines 13-28 overview; see, e.g., implementation details of pg. 13, line 19, to pg. 14, line 31)

altering the pixel to provide an indication that the message was opened by the recipient when the recipient opens the message and transmitting the message and the indication that the message was opened by the recipient to the server, (Tomkow, pg. 12, lines 13-28 overview; see, e.g., implementation details of pg. 13, line 19, to pg. 14, line 31, where, e.g., a unique visible element is added at server 14 for notification that the message has been opened by a recipient, followed by transmitting the message and pixel; see also further explanation in pg. 14, liens 23-31)

receiving the message, including the indication of the opening of the message the recipient, at the server, (Tomkow, see pg. 22, line 14 to pg. 25, line 2).

receiving an attachment at the server including an indication of the interim network stations which receive the message during the transmission of the message from the server to the recipient and back to the server, (Tomkow, see, e.g., pg. 5, lines 6-33 and pg. 22, line 14 to pg. 25, line 2, where the interim network stations are recorded and attached)

providing encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and transmitting to the sender the message, including the indication of the opening of the message the recipient, and the attachment, and the encrypted hashes of the message, including the opening of the message at the recipient, and the attachment (Tomkow, see pg. 22, line 14 to pg. 25, line 2, including the creation of an encrypted hash of the message with an indication of the opening of the message at the recipient; see also figs. 2E and 2F).

As per claim 8, Tomkow teaches the system further including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient, the attachment and the encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the messages, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash and the authenticity of the attachment on the basis of the hashed attachment and the hash decrypted from the encrypted hash of the attachment (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claims 9 and 15, Tomkow teaches the system further including the steps at the server of:

reviewing from the sender the message, including the indication of the opening of the message at the recipient, the encrypted hash of the message, including the indication of the opening of the message at the recipient, the attachment and the encrypted hash of the attachment, hashing the message, including the indication of the opening of the message the recipient, and the attachment to provide first digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachments, decrypting the encrypted hash of the message, including the indication of the opening of the message at the recipient, and the attachment to provide second digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachment, and comparing the first and second digital fingerprints of the message, including the indication of the opening of the message at the recipient, to determine the authenticity of the message, including the indication of the opening of the message at the recipient and first and second fingerprints of the attachment to determine the authenticity of the attachment (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claims 10 and 16, Tomkow teaches the system further including the steps at the server of:

indicating to the sender the results of the comparison, and disposing of the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, and the attachment and encrypted hash of the attachment when the message, the attachment and the encrypted hashes are transmitted by the server to the sender (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claim 11, Tomkow teaches the system further wherein the server receives the message from the sender through the internet and wherein the server transmits the message to the recipient through the internet and wherein the server re-transmits the message, including the indication of the opening of the message at the recipient, to the recipient through the internet and wherein the server transmits the message through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

As per claim 12, Tomkow teaches the system further wherein the server indicates the results of the comparison to the sender through the internet and wherein the server disposes of the message, the attachment and the encrypted hashes of the message and the attachment when the message and the encrypted hash are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

As per claim 14, Tomkow teaches the system further including the steps at the server of: receiving the message, the attachment and the encrypted hash of the combination of the message and the attachment from the sender, hashing the combination of the message and the attachment to provide a first digital fingerprint and decrypting the encrypted hash of the combination of the message and the attachment to form a second digital fingerprint, and determining the authenticity of the message and the attachment on the basis of the first and second digital fingerprints (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server, including where a first and second digital fingerprint of the message are created).

As per claims 17, Tomkow teaches the system further wherein the server receives the message from the sender through the internet, the server transmits the message to the recipient through the internet, the server receives the message, including the indication of the opening of the message the recipient, through the internet, and the server transmits the message, including the indication of the opening of the message at the recipient, through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

As per claims 18, Tomkow teaches the system further wherein the server disposes of the message, including the indication of the opening of the message at the internet, and the encrypted hash of the message, including the indication of the opening of the message, when the message and the encrypted hash are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

Conclusion

6. Applicant's amendment necessitated any new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicholas Taylor whose telephone number is (571) 272-3889. The examiner can normally be reached on Monday-Friday, 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571) 272-7493. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/NT/
Nicholas Taylor
Examiner
Art Unit 2441
/Larry D Donaghue/
Primary Examiner, Art Unit 2454